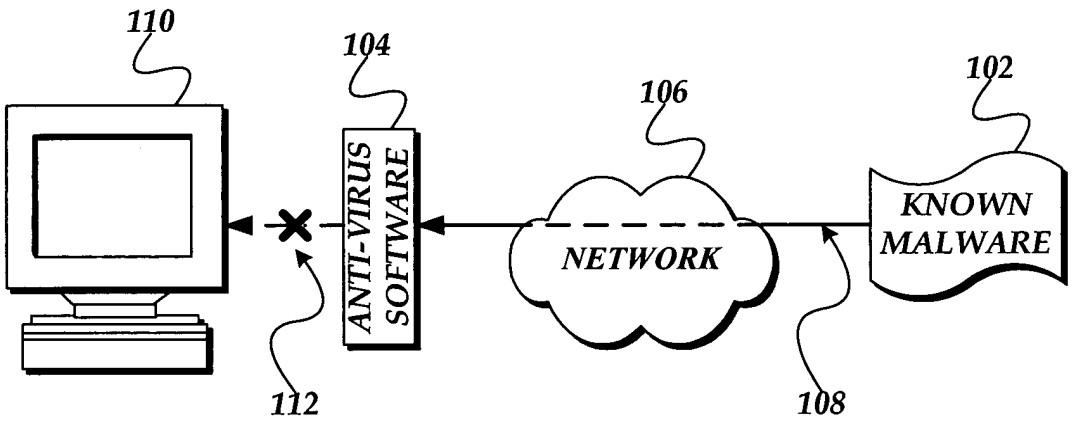

Fig.1A.
PRIOR ART

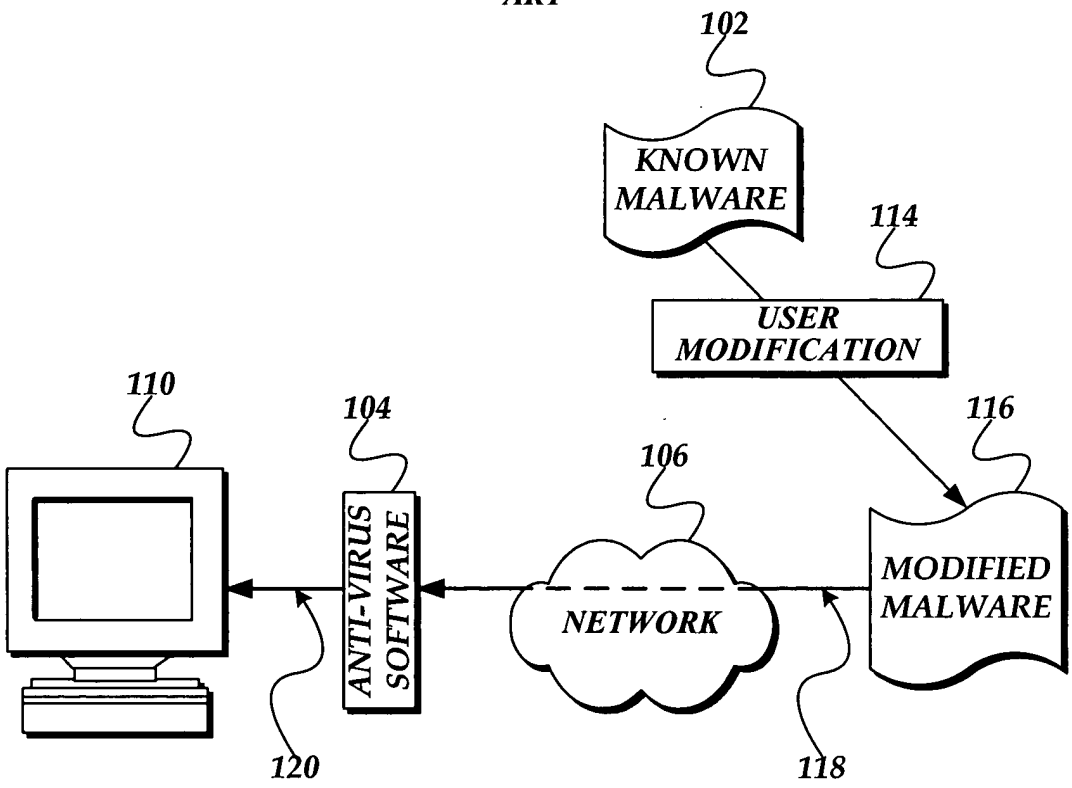

Fig.1B.
PRIOR ART

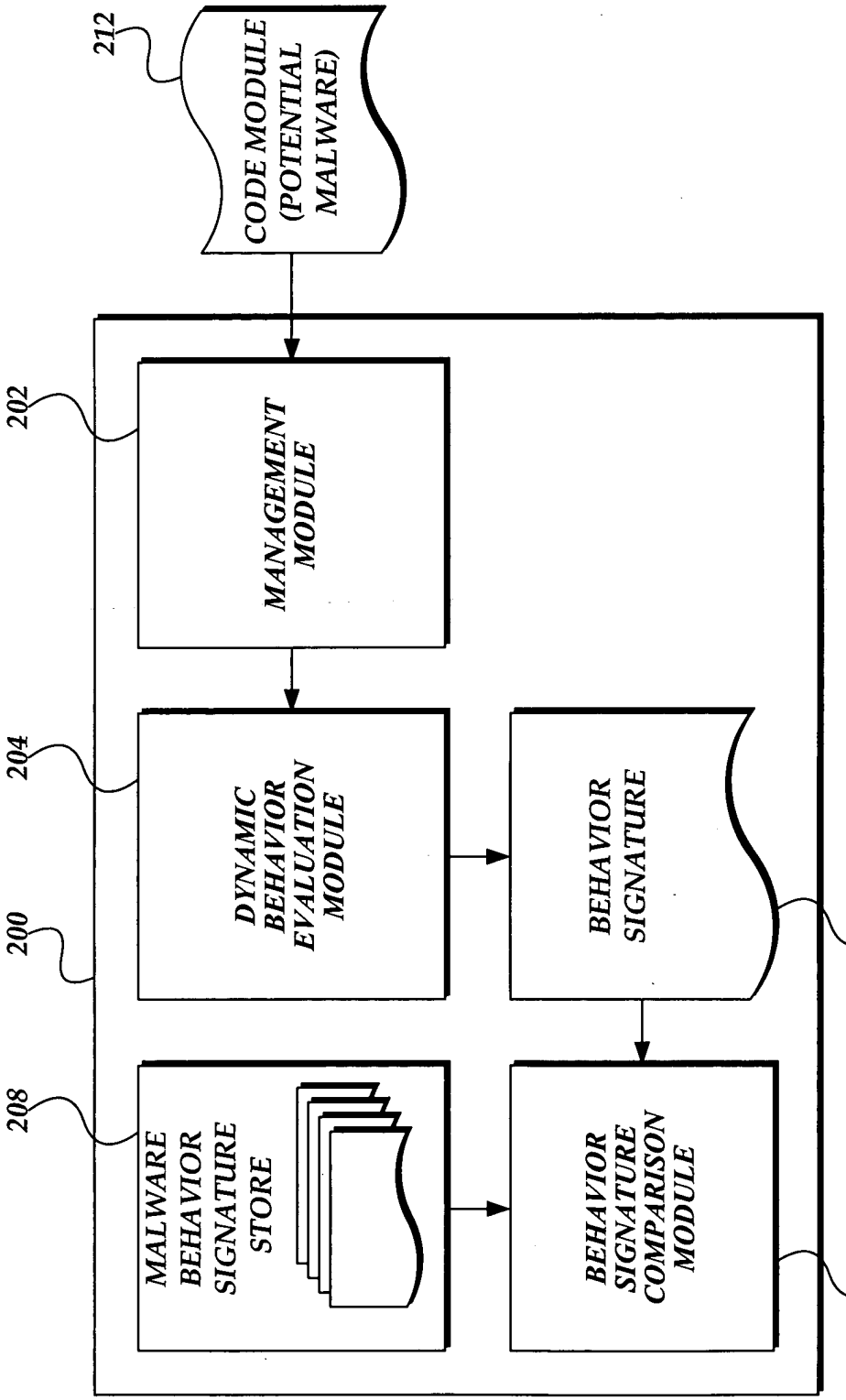
212
CODE MODULE (POTENTIAL MALWARE)
202
MANAGEMENT MODULE
204
DYNAMIC BEHAVIOR EVALUATION MODULE
200
BEHAVIOR SIGNATURE
210
208
MALWARE BEHAVIOR SIGNATURE STORE
BEHAVIOR SIGNATURE COMPARISON MODULE
206

Fig.2.

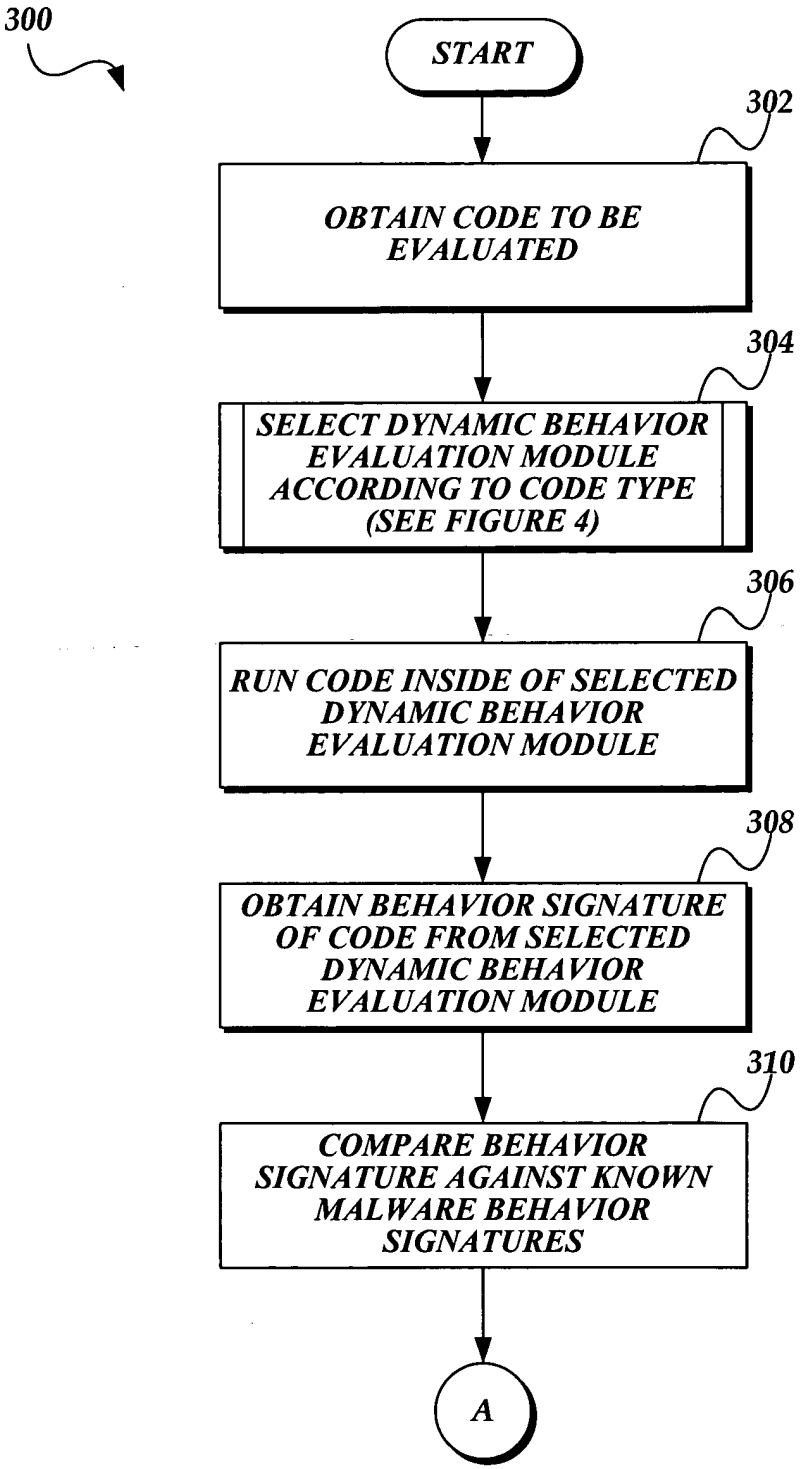
300
START
302
OBTAIN CODE TO BE EVALUATED
304
SELECT DYNAMIC BEHAVIOR EVALUATION MODULE ACCORDING TO CODE TYPE (SEE FIGURE 4)
306
RUN CODE INSIDE OF SELECTED DYNAMIC BEHAVIOR EVALUATION MODULE
308
OBTAIN BEHAVIOR SIGNATURE OF CODE FROM SELECTED DYNAMIC BEHAVIOR EVALUATION MODULE
310
COMPARE BEHAVIOR SIGNATURE AGAINST KNOWN MALWARE BEHAVIOR SIGNATURES
A

Fig.3A.

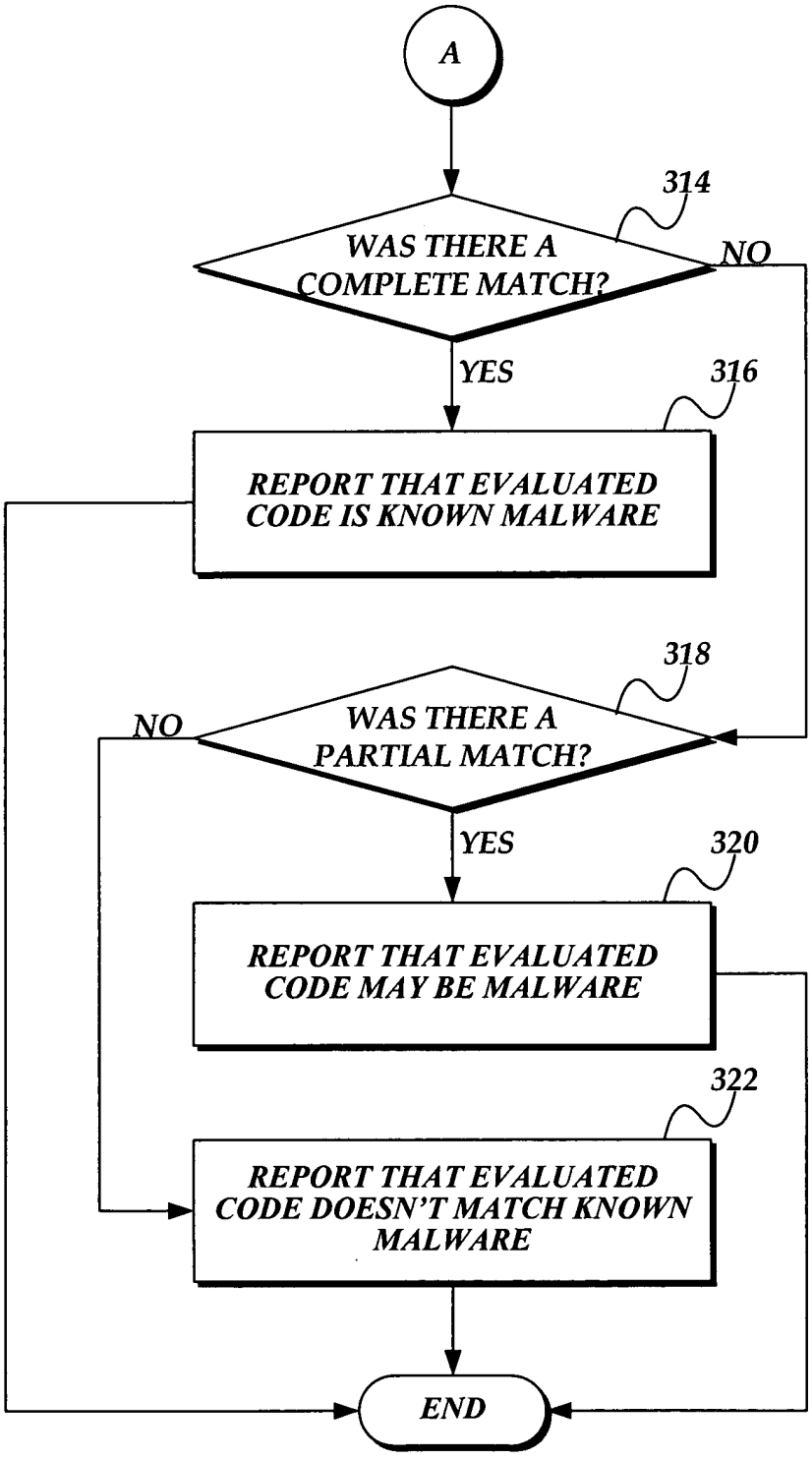
A
314
WAS THERE A COMPLETE MATCH?
NO
YES
316
REPORT THAT EVALUATED CODE IS KNOWN MALWARE
318
NO
WAS THERE A PARTIAL MATCH?
YES
320
REPORT THAT EVALUATED CODE MAY BE MALWARE
322
REPORT THAT EVALUATED CODE DOESN'T MATCH KNOWN MALWARE
END

Fig.3B.

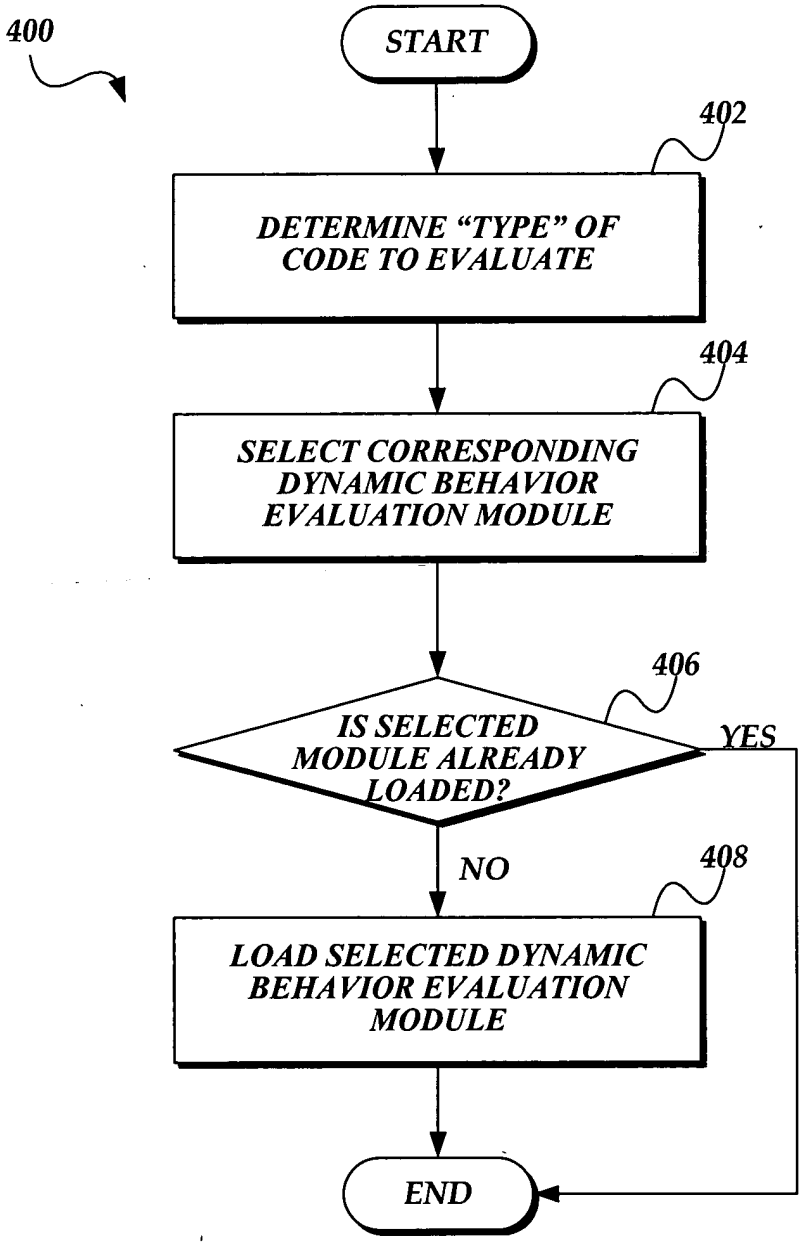
400
START
402
DETERMINE "TYPE" OF CODE TO EVALUATE
404
SELECT CORRESPONDING DYNAMIC BEHAVIOR EVALUATION MODULE
406
IS SELECTED MODULE ALREADY LOADED?
YES
NO
408
LOAD SELECTED DYNAMIC BEHAVIOR EVALUATION MODULE
END

Fig.4.

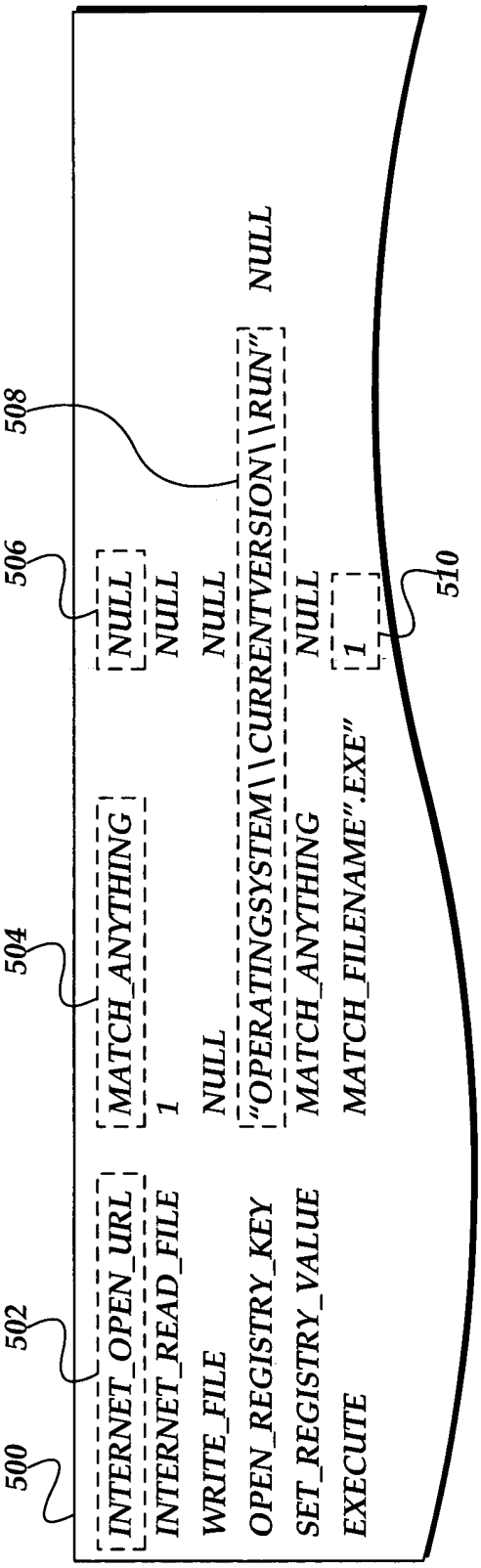
500
502
504
506
508
510
INTERNET_OPEN_URL
INTERNET_READ_FILE
WRITE_FILE
OPEN_REGISTRY_KEY
SET_REGISTRY_VALUE
EXECUTE
MATCH_ANYTHING
1
NULL
"OPERATINGSYSTEM\\CURRENTVERSION\\RUN"
MATCH_ANYTHING
MATCH_FILENAME".EXE"
NULL
NULL
NULL
NULL
NULL
1

Fig.5A.

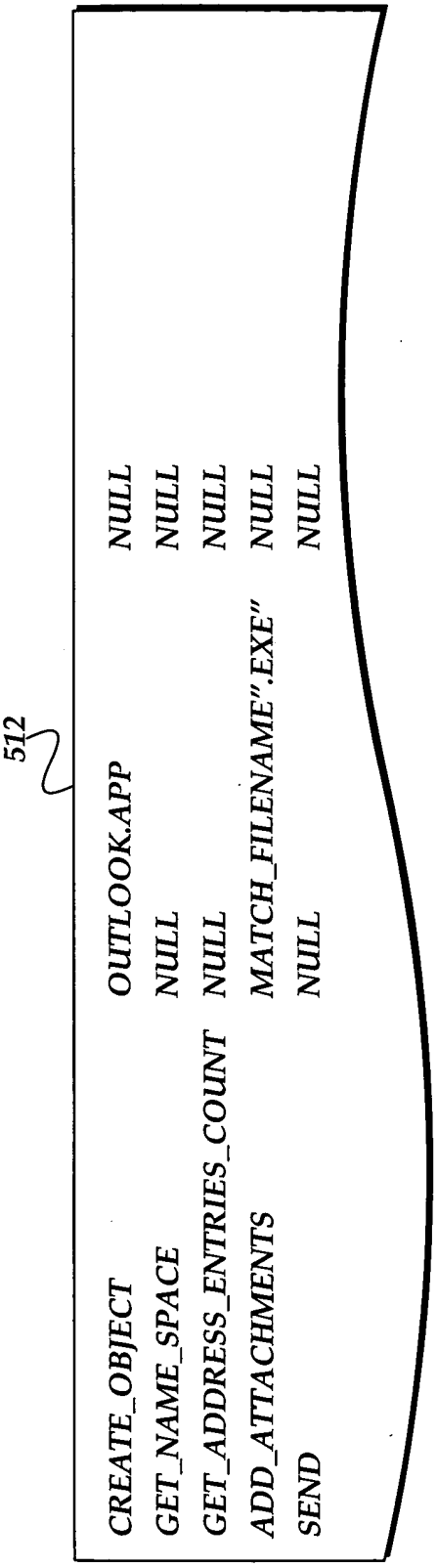
512
CREATE_OBJECT
GET_NAME_SPACE
GET_ADDRESS_ENTRIES_COUNT
ADD_ATTACHMENTS
SEND
OUTLOOK.APP
NULL
NULL
MATCH_FILENAME".EXE"
NULL
NULL
NULL
NULL
NULL

Fig.5B.